CLAIMS

1. A device for connection to a data processing apparatus, the device including means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information, and wherein the device controls access to the predetermined information.

2. The device of claim 1, comprising security data entry means for obtaining security data independently of the data processing apparatus, and means for analysing the entered security data for determining whether to allow access to the predetermined information.

3. The device of claim 2, wherein the security data entry means comprises alphanumeric data entry means.

4. The device of claim 2 or 3, wherein the security data entry means comprises a keypad.

5. The device of claim 2,3 or 4, wherein the security data comprises a Personal Identification Number (PIN) and the analysing means compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

6. The device of any one of the preceding claims, comprising a display for displaying security information.

7. The device of any one of the preceding claims, comprising a data processing module for controlling the communication with the data processing apparatus.

8. The device of claim 7, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

9. The device of claim 8, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

10. The device of claim 7,8 or 9, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module of the data processing apparatus.

11. The device of claim 7,8,9 or 10, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

12. The device of claims 10 or 11, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

13. The device of claim 12, wherein the key comprises a shared secret key for each of the respective data processing modules.

14. The device of any one of the preceding claims, wherein the device is operatively coupleable to one of more of a plurality of said authentication storage means, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the

telecommunications system.

15. The device of claim 14, in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

16. The device of claim 15, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

17. The device of any one of claims 1 to 16, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

18. The device of any one of claims 1 to 17, in which the authentication storage means is specific to that device.

19. The device of any one of claims 1 to 18, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

20. The device of any one of claims 14 to 19, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

21. The device of any one of the preceding claims in combination with the data processing apparatus.

22. The device of any one of the preceding claims in combination with the

telecommunications system.

23. A method for authenticating a transaction with data processing apparatus in which the data processing apparatus has operatively associated with it a security device which in turn has operatively associated with it authentication storage means for storing predetermined authentication information, and including the step of carrying out an authentication process via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined authentication information obtained from the authentication storage means via the security device which controls access to the predetermined authentication information.

24. The method of claim 23, comprising obtaining security data independently of the data processing apparatus, and analysing the security data for determining whether to allow access to the predetermined information.

25. The method of claim 24, wherein the security data is obtained by alphanumeric data entry means.

26. The method of claim 23 or 24, wherein the alphanumeric data entry means comprises a keypad.

27. The method of claim 24,25 or 26, wherein the security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

28. The method of any one of claims 23 to 27, comprising displaying security information.

29. The method of any one of claims 23 to 28, wherein communication with the data processing apparatus is controlled by a data processing module.

30. The method of claim 29, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

31. The method of claim 30, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

32. The method of claim 29,30 or 31, wherein the data processing module of the device decrypts encrypted data received from the data processing module of the data processing apparatus.

33. The method of claim 29,30, 31 or 32, wherein the data processing module of the device encrypts data transmitted to the data processing module of the data processing apparatus.

34. The method of claims 32 and 33, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

35. The method of claim 34, wherein the key comprises a shared secret key for each of the respective data processing modules.

36. A method according to any one of claims 23 to 35, wherein the security means is operatively associated with one or more authentication storage means of a plurality of authentication storage means each for storing predetermined authentication information, the authentication storage means being registerable with a common telecommunications

system, and wherein the step of carrying out the authentication process is performed via a communications link with the telecommunications system.

37. A method according to claim 36, in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

38. A method according to claim 37, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

39. A method according to any one of claims 37 to 38, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

40. A method according to any one of claims 23 to 39, in which each authentication storage is associated with a specific security device.

41. A method according to any one of claims 23 to 40, in which the authentication storage means is associated with the data processing apparatus by being associated with data or software for use by that data processing apparatus.

42. A method according to any one of claims 23 to 41, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

43. A method according to any one of claims 23 to 42, including the step of levying a

charge for the transaction when authenticated.

44. A method according to claim 43, in which the step of levying the charge is carried out by the said telecommunication system.

45. A method according to any one of claims 23 to 44, in which the data processing apparatus is a personal computer.

46. A device for controlling access to authentication data stored on a authentication storage means, the device including means for coupling the device to a data processing apparatus to allow the authentication data to be used to authenticate a transaction performed by the data processing apparatus, wherein security means is provided for controlling access to the authentication data via the data processing apparatus.

47. The device of claim 46, wherein the security means comprises means for obtaining security data from a user and means for checking the validity of the security data and only allowing access to the authentication data if the security data is valid.

48. The device of claim 46 or 47, wherein the security means comprises data processing means for receiving an encrypted authentication request, encrypted using a predetermined key, from the data processing apparatus and for decrypting the request.

49. The device of claim 48 in combination with the data processing means, wherein the data processing means comprises means for encrypting the authentication request using said key.

50. A device according to any one of claims 1 to 22 or 46 to 49, wherein the authentication storage means communicates wirelessly to authenticate the transaction.

51. A device according to claim 16, wherein the smart card or SIM authenticates the transaction when the smart card or SIM is operable in a mobile terminal.

52. A device according to claim 16, wherein the smart card or SIM is further operable to authenticate a mobile terminal for use in the system.

53. A method according to any one of claims 23 to 45, wherein the authentication storage means communicates wirelessly to authenticate the transaction.

54. A method according to claim 38, wherein the smart card or SIM authenticates the transaction when the smart card or SIM is operable in a mobile terminal.

55. A method according to claim 38, wherein the smart card or SIM is further operable to authenticate a mobile terminal for use in the system.